IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY OF SPACE ACTIVITIES (E9)
Cyber-based security threats to space missions: establishing the legal, institutional and collaborative framework to counteract them (2)

Author: Prof. Jyh-Ching Juang
National Cheng Kung University, Taiwan, China, juang@mail.ncku.edu.tw

LEAN SAT AND CONSTELLATION SECURITY

Abstract

Satellite systems have provided navigation, communication, and Earth observation data that are critically important to our society. The recent development in lean satellite paradigm aims to seek for affordable and effective access to space by streamlining the design, manufacturing, integration, test, and operation processes for the so-called modular commercial space system and constellation. It is noticed that space system cybersecurity remains an important issue in the procurement, design, implementation, and operation of satellites as well as satellite constellation. In the past, several incidents of cyber attacks on space assets have been reported. The lean satellite methodology cannot overlook cybersecurity, i.e., the security cannot be lean. To achieve an overall lean satellite design with a sufficient level of cyber security resilience, it is imperative to assess the development process, potential attacks, and resulting impacts. In the presentation, space cyberattacks are reviewed. Efforts in the standardization on space cybersecurity in the international community are reported. A cybersecurity maturity analysis framework for space system based on existing NIST framework is proposed in an attempt to tailor rigorous identify-protect-detect-respond-recover cycle and echo the lean satellite development spirit. A case study on the development of a university cubesat project and constellation security is then discussed.